Into the cloud, out of the fog

Ernst & Young’s 2011 Global Information Security Survey

December 2011
The Ernst & Young Global Information Security Survey is one of the longest running, most recognized and respected annual survey of its kind; for fourteen years our survey has helped our clients focus on the most critical risks, identify their strengths and weaknesses, and improve their information security.

This year, we conducted interviews with nearly 1,700 information security and IT leaders in 52 countries and across all industry sectors. Our 2011 results show that information security is still one of the most important issues facing our clients.
Introduction
Introduction

More and more businesses are moving into a virtual world, supported by new technologies and driven by a need to reduce costs. It is a fascinating journey into the “cloud” that these organizations have undertaken – one that we expect many more organizations will follow.

Our survey identifies three distinct trends that together have had and will continue to have a significant impact on the role and importance of information security.

First, a company’s physical boundaries are disappearing as more of its data is transmitted over the internet. Last year’s survey we already noted this development, and it continues to be a key area of concern.

Secondly, the pace of change continue to accelerate and have witnessed technology transform entire industries – from automotive to publishing to retail. The theme here is the move of business models that are increasingly “digital.”

Lastly, companies are moving from the more traditional outsourcing contracts to cloud service providers. As organizations realize the benefits of bringing their business into the cloud and confidence in the cloud business model continues to rise, they will move more critical capabilities and sometimes their entire IT infrastructure and applications platform into the cloud – thereby forever altering their business model and their IT functions.

Ernst & Young’s 2011 Global information Security Survey outlines these three trends, -- as well as other smaller ones impacting the role and importance of information security.

In Zimbabwe, we have also analysed our data with specific emphasis on issues pertaining to our environment.
Information Security and IT Risk Management

Information Security is one of the most important measures that an organization can take to potentially reduce IT Risks. However there are other areas that can be considered in reducing IT Risks.

IT risk has historically been dismissed as the sole responsibility of the IT Department and has not been considered as a strategic business risk requiring an enterprise-wide focus.

However as the pervasive use of IT tools and technology continues to grow, impacting virtually every aspect of the business function, it is becoming increasingly clear that managing IT risk is less about IT and more about managing risk for the whole business.

Organizations must now include IT Risk Management within their overall enterprise wide risk management approach.

The next slide shows the link between the business and IT risk management.
Evolvement of IT Risks over the years

The IT risk paradigm has always been subjected to changes but the complexity and types of risks have expanded significantly over the years and will continue to do so.
The Business Environment and IT Risk Management
The Business Environment and IT Risk Management (ITRM)

IT Risk Management remains an important enabler to achieving overall business objective. Organisations need to manage their “IT Risk Universe” to ensure that IT contributes positively to the business objective. ITRM provides the overall risk and control framework that enables the most important control framework for IT effectiveness, efficiency, compliance, confidentiality, integrity and availability.

It is clear that – with the exception of concerns about issues related to the start of the new millennium – IT risks are only increasing. The breadth and depth of the risks and the need for effective counter measures is expanding rapidly, and will likely to continue to accelerate. Many businesses are recognizing this: in our recent IT Risk Agenda Survey2, two-thirds agreed that managing IT risk has become more challenging over the past few years.

The growth of technologies such as mobile computing, cloud computing and virtualization, and the rapid adoption of social media platforms and online commerce/payments shows little sign of slowing. Newer technologies will continue to be created, each for these fast-moving companies, reliance on effective ITRM is considerable. They understand that an IT risk incident imperilling data and undermining consumer confidence could threaten their very existence. Cybercrime is a highly unpredictable risk and has inevitably drawn increasing governmental regulation and oversight scrutiny.

Survey Results on IT Megatrends

To address the evolving trends in IT risk and any critical categories within the IT Risk Universe, many organizations may need to do some significant re-evaluation or readjustment of their ITRM approach. IT should take into account not just the current state, but also factor in the future business response to the megatrends. In our survey, we asked executives in which categories of the IT Risk Universe they had experienced the most negative IT related incidents. Our results show that the three most commonly experienced incidents were in the categories of (1) security and privacy, (2) infrastructure and (3) data. It is not a surprise that all three categories also relate to most of the IT megatrends. We then also asked the participating executives if they planned to spend more or less on the different IT Risk Universe categories. Their response (see below) shows that:

- security and privacy and infrastructure are recognized as high risk areas and organizations are planning to spend more to mitigate these risks
- although applications and databases are not immediately a high risk category, organizations plan to spend more (with the potential risk of overspending)
- the risks around data are not yet very high on the corporate agenda (implying a potential risk of under spending).
Into the cloud, out of the fog
Survey results
Into the cloud, out of the fog - Global
Threat levels remain high as companies scramble to refine strategies to adjust to an ever-changing environment and the resulting security risks

72% of respondents see an increasing level of risk due to increased external threats.

In what way has the risk environment in which you operate changed in the last 12 months?

- We see an increasing level of risk due to increased (external) threats: 72%
- We see an increasing level of risk due to increased (internal) vulnerabilities: 46%
- We see a decreasing level of risk due to decreased (internal) vulnerabilities: 21%
- We see a decreasing level of risk due to decreased (external) threats: 9%
Into the cloud, out of the fog - Zimbabwe

Threat levels remain high as companies scramble to refine strategies to adjust to an ever-changing environment and the resulting security risks.

64% of respondents see an increasing level of risk due to increased external threats.

In what way has the risk environment in which you operate changed in the last 12 months?

- We see an increasing level of risk due to increased (external) threats: 64%
- We see a decreasing level of risk due to decreased (internal) vulnerabilities: 45%
- We see an increasing level of risk due to increased (internal) vulnerabilities: 34%
- We see a decreasing level of risk due to decreased (external) threats: 25%
59% of respondents expect their information security budget to increase over the next year.

In absolute terms, which of the following describes your organization's total planned information security budget in the coming 12 months?

- 59% Will increase
- 35% Will decrease
- 6% Will stay the same
Into the cloud, out of the fog - Zimbabwe
Resources are flowing into information security programs

82% of respondents expect their information security budget to increase over the next year. Zimbabwe is playing catch up in this area hence the proposed increases security budget.

In absolute terms, which of the following describes your organization's total planned information security budget in the coming 12 months?

- Will increase
- Will decrease
- Will stay the same

82%
While 49% of respondents stated that their information security function is meeting the needs of the organization, 51% said otherwise.

Do you believe the Information Security function is meeting the needs of your organization?

- Yes: 49%
- No, due primarily to budget constraints: 17%
- No, due primarily to a lack of skilled resources: 13%
- No, due to other reasons: 11%
- No, due primarily to a lack of executive support: 9%
Into the cloud, out of the fog - Zimbabwe
Despite efforts to grow the strength and capability of information security, a gap remains

While 41% of respondents stated that their information security function is meeting the needs of the organization, 59% said otherwise.

Do you believe the Information Security function is meeting the needs of your organization?

- Yes: 41%
- No, due primarily to budget constraints: 34%
- No, due primarily to a lack of skilled resources: 16%
- No, due primarily to a lack of executive support: 5%
- No, due to other reasons: 5%
Into the cloud, out of the fog

Our perspective

- Bring information security into the boardroom, making it more visible with a clearly defined strategy that will protect the business while also adding more value through tighter alignment with business needs.
- Make information security an integral part of service and product delivery and everyone’s day-to-day thinking.
- Focus information security on protecting what matters most, such as customer information and intellectual property. If information security is not adequate and not an enhancement to your brand, why should customers trust you as a business?
Keeping track of mobile computing
Survey results
Keeping track of mobile computing - Global
While personal adaptation rises, business use lags

20% of respondents indicated that their organization does not currently permit the use of tablets for business use, and has no plans to change that over the next year.

Does your organization currently permit the use of tablet computers for business use?

- Under evaluation or very limited use: 49%
- No, and no plans to use in the next 12 months: 20%
- Yes, widely in use and officially supported by the organization: 14%
- No, but planned within the next 12 months: 11%
- Yes, widely in use, but not officially supported by the organization: 9%
Keeping track of mobile computing - Zimbabwe
While personal adaptation rises, business use lags

37% of respondents indicated that their organization does not currently permit the use of tablets for business use, and has no plans to change that over the next year.

Does your organization currently permit the use of tablet computers for business use?

- No, and no plans to use in the next 12 months: 37%
- Under evaluation or very limited use: 33%
- No, but planned within the next 12 months: 14%
- Yes, widely in use and officially supported by the organization: 12%
- Yes, widely in use, but not officially supported by the organization: 5%
Keeping track of mobile computing - Global
As the use of tablets continues to rise, companies struggle to find ways to keep pace with the security concerns that come with them.

57% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of mobile computing?

- Policy adjustments: 57%
- Increased security awareness activities: 52%
- Encryption techniques: 47%
- Allow the use of company-owned tablets/smartphones, but disallow use of personal devices: 35%
- Architectural changes: 30%
- New mobile device management software: 28%
- Increased auditing capability: 27%
- Adjusted incident management processes: 26%
- New disciplinary processes: 13%
- None: 11%
- Disallow the use of all tablets / smartphones for professional use: 7%
Keeping track of mobile computing - Zimbabwe

As the use of tablets continues to rise, companies struggle to find ways to keep pace with the security concerns that come with them.

43% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.

<table>
<thead>
<tr>
<th>Control</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy adjustments</td>
<td>43%</td>
</tr>
<tr>
<td>Increased security awareness activities</td>
<td>43%</td>
</tr>
<tr>
<td>Encryption techniques</td>
<td>30%</td>
</tr>
<tr>
<td>Allow the use of company-owned tablets/smartphones, but disallow use of personal devices</td>
<td>30%</td>
</tr>
<tr>
<td>None</td>
<td>25%</td>
</tr>
<tr>
<td>New disciplinary processes</td>
<td>23%</td>
</tr>
<tr>
<td>Increased auditing capability</td>
<td>18%</td>
</tr>
<tr>
<td>Adjusted incident management processes</td>
<td>16%</td>
</tr>
<tr>
<td>Architectural changes</td>
<td>14%</td>
</tr>
<tr>
<td>New mobile device management software</td>
<td>9%</td>
</tr>
<tr>
<td>Disallow the use of all tablets / smartphones for professional use</td>
<td>7%</td>
</tr>
</tbody>
</table>
Keeping track of mobile computing

Our perspective

- Establish governance and guidance for the use of both mobile devices and their associated security software products.
- Use encryption as a fundamental control. Because fewer than half of the respondents are using it, organizations should consider embracing encryption.
- Perform attack and penetration testing on mobile apps before deployment to help reduce the organization’s risk exposure.
Seeing through the cloud
Survey results
Seeing through the cloud - Global
Even as cloud adoption rates and interest continue to climb, lack of clarity persists around security implications and measures.

61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.

Does your organization currently use cloud computing-based services?
Seeing through the cloud - Zimbabwe
Even as cloud adoption rates and interest continue to climb, lack of clarity persists around security implications and measures

25% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.

Does your organization currently use cloud computing-based services?

- Yes, currently in use: 7%
- Yes, under evaluation use: 5%
- No, but planned within the next 12 months: 14%
- No, and no plans within the next 12 months: 75%
Seeing through the cloud - Global
While cloud adoption rates and interest continue to climb, organizations’ information security efforts have not kept pace

More than half of the respondents have done almost nothing to mitigate new or increased risks related to the use of cloud computing

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of cloud computing?

<table>
<thead>
<tr>
<th>Control</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stronger oversight on the contract management process for cloud service providers</td>
<td>22%</td>
</tr>
<tr>
<td>Increased due diligence of service providers</td>
<td>21%</td>
</tr>
<tr>
<td>Stronger identity and access management controls</td>
<td>19%</td>
</tr>
<tr>
<td>Encryption techniques</td>
<td>18%</td>
</tr>
<tr>
<td>Onsite inspection by your security / IT risk team</td>
<td>16%</td>
</tr>
<tr>
<td>Increased auditing of cloud service provision</td>
<td>15%</td>
</tr>
<tr>
<td>More reliance on 3rd party certification of cloud service providers</td>
<td>13%</td>
</tr>
<tr>
<td>Contracting with a 3rd party to test controls at a cloud service provider</td>
<td>13%</td>
</tr>
<tr>
<td>Increased liability for cloud service providers in contracts</td>
<td>11%</td>
</tr>
<tr>
<td>Adjusted incident management processes</td>
<td>11%</td>
</tr>
<tr>
<td>Financial penalties in the case of security breaches</td>
<td>8%</td>
</tr>
</tbody>
</table>
Seeing through the cloud - Zimbabwe

While cloud adoption rates and interest continue to climb, organizations’ information security efforts have not kept pace

Almost three quarters of the respondents have done almost nothing to mitigate new or increased risks related to the use of cloud computing

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of cloud computing?

- None: 73%
- Stronger identity and access management controls: 20%
- Encryption techniques: 10%
- Onsite inspection by your security / IT risk team: 10%
- Increased due diligence of service providers: 5%
- Increased auditing of cloud service provision: 2%
- More reliance on 3rd party certification of cloud service providers: 2%
- Contracting with a 3rd party to test controls at a cloud service provider: 2%
- Increased liability for cloud service providers in contracts: 2%
- Adjusted incident management processes: 2%
- Financial penalties in the case of security breaches: 2%
- Stronger oversight on the contract management process for cloud service providers: 2%
Seeing through the cloud

Our perspective

- Choose verification above trust.
- Understand who owns the risks before entering a cloud agreement.
- Plan for continuity and select providers that are transparent about resiliency build backups and test recoverability.
- Proceed in using the standard security processes and techniques that have worked effectively on other technologies in the past.
- Align your business and information security strategy, and continuously assess risks to comply with regulations and industry standards.
Connecting with social media
Survey results
Connecting with social media - Global
Organizations are trying to figure out the best way forward to help address security threats in an open, dynamic and nascent industry that is impacting almost every facet of business.

53% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of social media?

- Limited or no access to social media sites: 53%
- Policy adjustments: 46%
- Security & social media awareness programs: 39%
- Enhanced internet use monitoring: 38%
- New disciplinary processes: 12%
- Adjusted incident management processes: 11%
- None: 15%
Connecting with social media - Zimbabwe
Organizations are trying to figure out the best way forward to help address security threats in an open, dynamic and nascent industry that is impacting almost every facet of business.

64% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.

Which of the following controls have you implemented to mitigate the new or increased risks related to the use of social media?

- Limited or no access to social media sites: 64%
- Enhanced internet use monitoring: 52%
- Policy adjustments: 36%
- Security & social media awareness programs: 25%
- New disciplinary processes: 16%
- Adjusted incident management processes: 16%
- None: 14%
Connecting with social media

Consider using hard-and-fast “no access/no use” policies for social media sites. This response, while perhaps addressing external threats to internal hardware and software, does not completely address the widespread global personal adoption of social media usage and indirect integration into business use via other channels such as mobile devices. Organizations may consider monitoring their employees’ usage of these sites, without restricting access.

Embrace the full advantages of social media. The lack of an integrated information security policy for both access to and use of social media is preventing companies from keeping pace with competitors and may be creating a sense of mistrust with employees.

Perform your own reconnaissance to better understand what potential attackers can find on social media.
Plugging the data leaks
Survey results
Plugging the data leaks - Global
Organizations are moving ahead with policies, procedures and awareness campaigns to help identify holes through which data can pour, but whether it’s enough is unclear.

66% of respondents have not implemented data loss prevention (DLP) tools. These are systems that identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination and so on) and with a centralized management framework.

Regarding DLP tools implementation, how would you describe that deployment?

- We have not implemented DLP tools: 66%
- Users have largely not noticed the impact of these tools: 15%
- Our implementation has been a success: 14%
- Implementation has gone smoothly and according to schedule: 14%
- It has taken longer than expected to implement: 12%
- Users have been upset with the impact to their daily routines: 6%
- Our implementation has not been as successful as expected thus far: 4%
55% of respondents have not implemented data loss prevention (DLP) tools.

Regarding DLP tools implementation, how would you describe that deployment?

- We have not implemented DLP tools: 55%
- Our implementation has been a success: 30%
- Implementation has gone smoothly and according to schedule: 25%
- Users have largely not noticed the impact of these tools: 18%
- Users have been upset with the impact to their daily routines: 13%
- It has taken longer than expected to implement: 8%
- Our implementation has not been as successful as expected thus far: 3%
Plugging the data leaks - Global
Organizations are relying mostly on policies and programs as their first line of defense against data loss and leakage

74% of respondents have defined a policy for classification and handling sensitive data as control for data leakage risk.

<table>
<thead>
<tr>
<th>Action</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined a specific policy regarding the classification and handling of sensitive information</td>
<td>74%</td>
</tr>
<tr>
<td>Employee awareness programs</td>
<td>69%</td>
</tr>
<tr>
<td>Implemented additional security mechanisms for protecting information (e.g., encryption)</td>
<td>60%</td>
</tr>
<tr>
<td>Looked down/restricted use of certain hardware components (e.g., USB drives or FireWire ports)</td>
<td>45%</td>
</tr>
<tr>
<td>Utilized internal auditing for testing of controls</td>
<td>45%</td>
</tr>
<tr>
<td>Defined specific requirements for telecommuting/telework regarding protection of information taken outside office</td>
<td>43%</td>
</tr>
<tr>
<td>Implemented log review tools</td>
<td>39%</td>
</tr>
<tr>
<td>Implemented data loss prevention tools (McAfee, Symantec, Verdasys, etc.)</td>
<td>38%</td>
</tr>
<tr>
<td>Restricted or prohibited use of instant messaging or email for sensitive data transmission</td>
<td>35%</td>
</tr>
<tr>
<td>Prohibited use of camera devices within sensitive or restricted areas</td>
<td>24%</td>
</tr>
<tr>
<td>Restricted access to sensitive information to specific time periods</td>
<td>15%</td>
</tr>
</tbody>
</table>
### Plugging the data leaks - Zimbabwe

Organizations are relying mostly on policies and programs as their first line of defense against data loss and leakage.

64% of respondents have defined a policy for classification and handling sensitive data as control for data leakage risk.

---

Which of the following actions has your organization taken to control data leakage of sensitive information?

<table>
<thead>
<tr>
<th>Action</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined a specific policy regarding the classification and handling of sensitive information</td>
<td>64%</td>
</tr>
<tr>
<td>Implemented data loss prevention tools (McAfee, Symantec, Verdasys, etc.)</td>
<td>61%</td>
</tr>
<tr>
<td>Utilized internal auditing for testing of controls</td>
<td>57%</td>
</tr>
<tr>
<td>Implemented additional security mechanisms for protecting information (e.g., encryption)</td>
<td>48%</td>
</tr>
<tr>
<td>Implemented log review tools</td>
<td>41%</td>
</tr>
<tr>
<td>Locked down/restricted use of certain hardware components (e.g., USB drives or FireWire ports)</td>
<td>39%</td>
</tr>
<tr>
<td>Defined specific requirements for telecommuting/ telework regarding protection of information taken outside office</td>
<td>16%</td>
</tr>
<tr>
<td>Restricted or prohibited use of instant messaging or email for sensitive data transmission</td>
<td>16%</td>
</tr>
<tr>
<td>Restricted access to sensitive information to specific time periods</td>
<td>11%</td>
</tr>
<tr>
<td>Prohibited use of camera devices within sensitive or restricted areas</td>
<td>9%</td>
</tr>
</tbody>
</table>
Plugging the data leaks

- Assess, understand and appreciate the many potential risks and areas of data loss, specifically relating to the data loss channels that exist within the organization.
- Identify, assess and classify sensitive data so that DLP controls can be focused to provide protection for the most sensitive data.
- Take a holistic view of data loss prevention by identifying key DLP controls and measuring their effectiveness. All key controls, such as asset management and physical security controls, should provide accurate reporting of data loss risks and controls.
- Cover data in motion, data at rest and data in use within the organization’s DLP controls.
- Implement incident investigation, enlist a strong team to carry out the program and seek the support of key stakeholders.
- Pay special attention to third parties with access to sensitive company data.
- Understand what data is sent to third parties, how it is sent and if the transmission mechanisms are secure.
Preparing for the worst
Survey results
Preparing for the worst
Business continuity continues to be a top funding priority

Nearly three times the number of respondents rated BCM a higher funding priority than their second-ranked priority.

Which of the following information security areas will receive the most funding over the coming 12 months?

<table>
<thead>
<tr>
<th>Area</th>
<th>1st priority</th>
<th>2nd priority</th>
<th>3rd priority</th>
<th>4th priority</th>
<th>5th priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity/disaster recovery plans and capabilities</td>
<td>30%</td>
<td>8%</td>
<td>7%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Data leakage/data loss prevention technologies and processes</td>
<td>15%</td>
<td>10%</td>
<td>6%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Compliance monitoring (to internal &amp; external policies and standards)</td>
<td>10%</td>
<td>11%</td>
<td>8%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Identity and access management technologies and processes</td>
<td>9%</td>
<td>12%</td>
<td>9%</td>
<td>8%</td>
<td>6%</td>
</tr>
<tr>
<td>Securing new technologies (e.g., cloud computing, virtualization, mobile)</td>
<td>6%</td>
<td>8%</td>
<td>9%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Information security risk management</td>
<td>5%</td>
<td>8%</td>
<td>10%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Implementing security standards (e.g., ISO/IEC 27002:2005)</td>
<td>4%</td>
<td>5%</td>
<td>5%</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Security testing (e.g., attack and penetration)</td>
<td>3%</td>
<td>0%</td>
<td>6%</td>
<td>11%</td>
<td>8%</td>
</tr>
<tr>
<td>Vulnerability management technologies and processes</td>
<td>11%</td>
<td>8%</td>
<td>6%</td>
<td>8%</td>
<td>9%</td>
</tr>
<tr>
<td>Security awareness and training</td>
<td>0%</td>
<td>5%</td>
<td>7%</td>
<td>8%</td>
<td>11%</td>
</tr>
<tr>
<td>Outsourcing security functions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response plans and capabilities</td>
<td>4%</td>
<td>6%</td>
<td>5%</td>
<td>8%</td>
<td></td>
</tr>
<tr>
<td>Forensics/fraud support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure development processes (e.g., secure coding, QA process)</td>
<td>4%</td>
<td>5%</td>
<td>3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security performance management (e.g., metrics and reporting)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recruiting security resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This key hangs way out over the edge. Can we redo this graphic or use the one used in the report?

Author, 2011/10/24
Preparing for the worst - Global

While the focus on business continuity - and the resources to support it - continues to be a top priority, most companies are still unprepared for catastrophic occurrence.

For the second consecutive year, respondents have indicated that business continuity is their top funding priority.

Which of the following statements apply to your organization’s Business Continuity Management (BCM) strategy and program?

- Our BCM program is approved by management: 50%
- We have incident and crisis management procedures in place: 55%
- We have procedures to enable the continuity of the ICT infrastructure (e.g., ICT Disaster Recovery Plan): 55%
- We have procedures in place to enable the continuity of critical business processes: 55%
- We have procedures to protect our organization’s people (e.g., evacuation plans, influenza pandemic response plans): 55%
- Our BCM program covers all critical business processes: 53%
- We continuously improve our BCM program: 49%
- We have identified the required recovery time for business critical resources (e.g., through a Business Impact Analysis): 49%
- Our BCM program is well documented and includes policies, processes, roles and responsibilities: 47%
- We continuously identify and assess key business continuity threats and risks: 39%
- We have established relationships with local emergency response groups (e.g., fire fighters, police, emergency teams): 38%
- We continuously monitor and report on BCM related risks, issues, program status, and initiatives: 33%
- We do not have a business continuity management program in place: 18%
Preparing for the worst - Zimbabwe
While the focus on business continuity - and the resources to support it - continues to be a top priority, most companies are still unprepared for catastrophic occurrence

Respondents have indicated that business continuity is their top funding priority.

Which of the following statements apply to your organization’s Business Continuity Management (BCM) strategy and program?

- We do not have a business continuity management program... 19%
- We have established relationships with local emergency services... 26%
- We have procedures in place to protect our ICT infrastructure... 30%
- We have identified the required recovery time for our operations... 28%
- We have procedures in place to enable the continuity of our business processes... 26%
- We have incident and crisis management procedures in place... 30%
- We continuously identify and assess key business risks... 44%
- We continuously improve our BCM program... 42%
- Our BCM program is approved by management... 42%
- Our BCM program is well documented and includes procedures... 37%
- Our BCM program covers all critical business processes... 37%
- We continuously monitor and report on BCM related metrics... 33%
- We have procedures to enable the continuity of the ICT infrastructure... 77%
Preparing for the worst

- Prepare for and secure business continuity plans that anticipate high-impact, low-frequency events, and determine which are integrated into a broader risk management framework that focuses on protecting the organization from catastrophic loss.
- Assess whether the business continuity plan has the right level of maturity in light of the emerging trends and new technologies.
- Test the organization’s business continuity plan frequently to help validate your business resiliency in practice. The more complex the scenarios that are tested, the better the coverage of the test.
- Solicit the support of the board and the audit committee for their business continuity programs.
- There is need for Zimbabwe to consider elevating business continuity management to executives and boards.
- We lag in incident and skills management
Looking into the future
Survey results
Looking into the future - Global
Many companies are approaching information security without a plan

Does your organization have a documented information security strategy for the next one to three years?

Nearly half of the responding organizations do not have an information security strategy.
Looking into the future - Zimbabwe
Many companies are approaching information security without a plan

Does your organization have a documented information security strategy for the next one to three years?

- No: 36%
- Yes: 64%
Looking into the future - Global

Just over a third of organizations do not have an information security strategy, and for the rest, plans continue to evolve despite a sense they may not be effective.

56% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.

Which of the following statements best describes your organization’s information security strategy in relation to today’s threat landscape?

- 43%: Our current information security strategy adequately addresses the risks
- 33%: We need to modify our strategy to address the new risks
- 23%: We need to investigate further to understand the risks
- 33%: We do not see any new or increased risks
Looking into the future - Zimbabwe

Nearly half of organizations do not have an information security strategy, and for the rest, plans continue to evolve despite a sense they may not be effective.

84% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.

Which of the following statements best describes your organization’s information security strategy in relation to today’s threat landscape?

- 55%: Our current information security strategy adequately addresses the risks
- 29%: We need to modify our strategy to address the new risks
- 16%: We need to investigate further to understand the risks
- 0%: We do not see any new or increased risks associated with these technologies
Looking into the future - Global

Nearly a third of respondents indicate that they have bought solutions which they later felt failed or under-performed.

31% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Has your organization purchased software and/or hardware to support information security initiatives in the past 18 months which is perceived as having failed or under-delivered?

- Yes: 69%
- No, all of our information security technology has been successfully implemented: 31%
Looking into the future - Zimbabwe
Nearly one fifth of respondents indicate that they have bought solutions which they later felt failed or under-performed

20% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.

Has your organization purchased software and/or hardware to support information security initiatives in the past 18 months which is perceived as having failed or under-delivered?

- 20%
- 80%
Looking into the future - Global
Most companies recognize the importance of having an IT risk management plan

84% of respondents indicated that they have an IT risk management program in place or are considering it within the coming year.

Do you have a formalized IT risk management program in place at your organization?

- Yes, we have an IT risk management program that has existed for less than three years (31%)
- No, but considering it within the coming 12 months (25%)
- Yes, we have had a well-established IT risk management program in place for more than three years (28%)
- No, and not considering it (16%)
Looking into the future - Zimbabwe
Most companies recognize the importance of having a IT risk management plan

89% of respondents indicated that they have an IT risk management program in place or are considering it within the coming year.

Do you have a formalized IT risk management program in place at your organization?

- Yes, we have had a well-established IT risk management program in place for more than three years (11%)
- Yes, we have an IT risk management program that has existed for less than three years (18%)
- No, but considering it within the coming 12 months (25%)
- No, and not considering it (45%)
Looking into the future

- Revisit your information security strategy to conform to the current risk landscape.
- Instead of acquiring the latest tools, focus on the fundamentals.
- Implement a structured, pragmatic approach to managing IT risk to make sure it focuses on the risks that matter. We see an IT risk management or governance risk and compliance (GRC) approach as a key future investment for many organizations.
- Address the entire IT risk universe in your IT risk or GRC program, which is broader than just information security.
Summary of survey findings
# Key survey findings - Global

| Introduction | 72% of respondents see an increasing level of risk due to increased external threats.  
|             | 49% of respondents stated that their information security function is meeting the needs of the organization. |
| Cloud computing | 61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.  
|             | Almost 90% of respondents believe that external certification would increase their trust in cloud computing. |
| Mobile computing | 80% of respondents are either planning, evaluating or actually using tablet computers.  
|             | 57% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks. |
| Social media | Nearly 40% of respondents rated social media-related risks issues as challenging.  
|             | 53% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media. |
| Data loss prevention | 66% of respondents have not implemented data loss prevention tools.  
|             | 74% of respondents have defined a policy for classification and handling of sensitive data as a control for data leakage risk. |
| Business continuity management | For the second consecutive year, respondents have indicated that business continuity is their top funding priority. |
| IT risk management | 56% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.  
|             | 31% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered. |
### Key survey findings - Zimbabwe

<table>
<thead>
<tr>
<th>Introduction</th>
<th>64% of respondents see an increasing level of risk due to increased external threats.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>41% of respondents stated that their information security function is meeting the needs of the organization.</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>25% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year.</td>
</tr>
<tr>
<td></td>
<td>Almost 20% of respondents believe that external certification would increase their trust in cloud computing.</td>
</tr>
<tr>
<td>Mobile computing</td>
<td>76% of respondents are either planning, evaluating or actually using tablet computers.</td>
</tr>
<tr>
<td></td>
<td>43% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks.</td>
</tr>
<tr>
<td>Social media</td>
<td>Nearly 45% of respondents rated social media-related risks issues as challenging.</td>
</tr>
<tr>
<td></td>
<td>64% of respondents have implemented limited or no access to social media sites as a control to mitigate risks related to social media.</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>55% of respondents have not implemented data loss prevention tools.</td>
</tr>
<tr>
<td></td>
<td>64% of respondents have defined a policy for classification and handling of sensitive data as a control for data leakage risk.</td>
</tr>
<tr>
<td>Business continuity management</td>
<td>66% Most respondents have indicated that business continuity is their top funding priority.</td>
</tr>
<tr>
<td></td>
<td>84% of respondents indicated that their current information security strategy needs to be modified or needs further investigation.</td>
</tr>
<tr>
<td>IT risk management</td>
<td>20% of respondents indicated that their organization has recently purchased information security solutions that are perceived as having failed or under-delivered.</td>
</tr>
</tbody>
</table>
Other survey findings - Zimbabwe

Areas where are ahead of other firms - globally

- We are spending more (23%) on information security compared to other firms globally. This is because we are playing catch up for the period where there was little investments in IT and related risks. This figure is 10% higher than what companies spend last year.

- Globally firms top priority is spending on BCM and this is consistent with Zimbabwe although Zimbabwe is ahead on this metric by about 10%.

- Also 75% of Zimbabwe companies will spend more on data loss prevention technologies for the same reason mentioned above.

- The area likely to get least funding is forensics, likely because of the specialist skills required and that this service will be bought outside.

- More companies will spend on the implementation of standards. Areas likely to get the most funding are CoBIT, ISO 27002 and ITIL.

- 92% of companies have planned to carry out security testing in the coming 12 months (e.g. Attack & penetration exercise).

- 93% of companies indicated they will take time to look at emerging trends in IT and adopt based on relevance with 74% perceiving a challenge with the adoption of new technologies.

- 80% of respondents indicate the budget is one of their greatest challenges with regards to the implementation of IT risk management solutions.

- 66% see a challenge in the uncertainty of the business environment.

- Increased used of tablet computers, smart-phones and other mobile services is perceived to be posing a challenge to 67% of the respondents.

- 95% of respondent plan to implement data loss prevention tools.
Other survey findings - Zimbabwe

Areas where we are lagging other firms - globally

- Zimbabwean companies under estimate the internal threat compared with other companies globally (45% vs. 21%)
- We also lag in the following best practices in terms of controlling data losses due to mobile computing:
  - Encryption techniques (30% usage for Zim vs. 46% globally)
  - Architectural changes (14% usage for Zim vs. 30% globally)
  - Adjusted incident management processes (26% usage for Zim vs. 16% globally)
  - Mobile device management software (28% usage for Zim vs. 9% globally)
  - Policy adjustments (57% usage for Zim vs. 43% globally)
- We also lag on our security and awareness programs as it relates to social media (by 14%)
- We lag in the following with regards to data loss:
  - Defining policies regarding information that is taken outside the office (lagging by 27%)
  - Restricted the transmission of sensitive information through email / instant messaging (lagging by 19%)
  - Defining security policies for protection of information (lagging by 12%)
  - Laptop and desktop encryption (lagging by 33% and 14% respectively)
- In terms of testing of the networks, we lag in the following:
  - External networking vulnerability scanning and penetration testing lagging by 21%
  - Application layer security testing (lagging by 10%)
- We are lagging the rest of the world in establishing ITRM functions by about 12%.
- Our BCM lags in the following areas: protecting our people (27% lagging); incident and crisis management procedures (25%); Recovery Time Objectives (19%) and inclusion of all business processes (16%).
Transforming your security program
Our services
Transform your security program to improve business performance

Identify the real risks

Protect what matters most

Enable business performance

Sustain an enterprise program

Optimize for business performance

Five questions for the C-suite

► Do you know how much damage a security breach can do to your reputation or brand?

► Are internal and external threats considered when aligning your security strategy to your risk management efforts?

► How do you align key risk priorities in relation to your spending?

► Do you understand your risk appetite and how it allows you to take controlled risks?

► How does your IT risk management strategy support your overall business strategy?
Framework to enable your security program to address business needs

Integrated capabilities

Security methods and processes

Security risk governance & risk management

Business-level performance

Key business drivers

External challenges

Integrated security program
Ernst & Young information security services are focused on sustainable business improvement solutions

### Accelerators

- **Business and industry sector focus**
- **Technical research through Advanced Security Centers**
- **Diverse personnel who drive fact-based, creative business improvement**
- **Proprietary frameworks, tools and thought leadership**
- **Most globally aligned of the Big Four with an award-winning people culture**

### Client outcomes

<table>
<thead>
<tr>
<th>Assess</th>
<th>Transform</th>
<th>Sustain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security program management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security strategy and road map</td>
<td>Security reporting and metrics</td>
<td></td>
</tr>
<tr>
<td>Organization and governance</td>
<td>Business continuity management</td>
<td></td>
</tr>
<tr>
<td>Information security risk assessment</td>
<td>Third-party risk management</td>
<td></td>
</tr>
<tr>
<td><strong>Threat and vulnerability management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack and penetration</td>
<td>Application testing and secure SDLC</td>
<td></td>
</tr>
<tr>
<td>Cyber security investigations</td>
<td>Control system security</td>
<td></td>
</tr>
<tr>
<td>Vulnerability management</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Identity and access management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy and governance</td>
<td>Review and certification</td>
<td></td>
</tr>
<tr>
<td>Request and approval</td>
<td>Role and rules management</td>
<td></td>
</tr>
<tr>
<td>Provisioning and de-provisioning</td>
<td>Reconciliation</td>
<td></td>
</tr>
<tr>
<td>Enforcement</td>
<td>Reporting and analytics</td>
<td></td>
</tr>
<tr>
<td><strong>Information protection and privacy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data protection strategy</td>
<td>Data loss prevention</td>
<td></td>
</tr>
<tr>
<td>Privacy implementation design</td>
<td>Privacy assessment and remediation</td>
<td></td>
</tr>
</tbody>
</table>

### Accelerators

- **Assess**
  - Security program management
  - Threat and vulnerability management
  - Identity and access management
  - Information protection and privacy

- **Transform**
  - Security strategy and road map
  - Organization and governance
  - Information security risk assessment
  - Attack and penetration
  - Cyber security investigations
  - Vulnerability management
  - Application testing and secure SDLC
  - Control system security
  - Strategy and governance
  - Request and approval
  - Provisioning and de-provisioning
  - Enforcement
  - Review and certification
  - Role and rules management
  - Reconciliation
  - Reporting and analytics
  - Data protection strategy
  - Privacy implementation design
  - Data loss prevention
  - Privacy assessment and remediation

- **Sustain**
  - Security reporting and metrics
  - Business continuity management
  - Third-party risk management
  - Application testing and secure SDLC
  - Control system security
  - Review and certification
  - Role and rules management
  - Reconciliation
  - Reporting and analytics
  - Data loss prevention
  - Privacy assessment and remediation

### Client outcomes

- Transformed security program driving business performance
- Integrated information security and IT risk approach across enterprise
- Identified and evaluated internal and external threats
- Optimized measures to mitigate threats
- Understand who has or needs access to important data and applications
- Sustainable, compliant and efficient access processes
- Protect information that matters and detect leakage
- Regulatory and industry compliance
Related Insights
To see these and more, visit www.ey.com
Related Insights

**Business continuity management**

Only about half of companies have taken steps to address these potential disruptions and disasters. Organizations need to develop, maintain and sustain effective business continuity management programs.

**Information security in a borderless world**

Traditional security models that focus primarily on keeping the bad guys out no longer work. It’s time to radically rethink how organizations can keep their most valuable assets safe.

**The evolving IT risk landscape**

A strategic IT risk management program helps address IT risks consistent with strategic corporate objectives and help set risk culture by providing management with a holistic, enterprise-wide perspective.

**Mobile device security**

New mobile technologies come with new risks that are specific to the various device platforms and technologies. These risks may be mitigated through technical device controls, third-party software, and organizational policy.

**Countering cyber attacks**

Given the continuous and persistent threat posed by new waves of attack channels and malicious entities, leading companies recognize the need to instill a new mind-set and approach toward the organization’s security strategy.

**Cloud computing: Issues and impacts**

Cloud computing alters the technology industry power structure, and can improve business agility and access to computing, storage and communications power.

**Data loss prevention: Keeping your data safe**

Advances in technology and how users apply that technology, has increased the risk of data leakage. The blurry line between work and personal use of – and access to – data can result in unintentional leaks, as well as malicious ones.

**Building confidence in IT programs**

About two out of three large IT programs go over budget, are completed too late or do not deliver the expected benefits. Having the right information at the right time can help build confidence throughout the program lifecycle.
Contact Information
For any information on the survey and our services, please contact the following people:
Contact Details

Leonard Bore
IT Risk & Assurance (ITRA) Partner
Email Address: leonard.bore@zw.ey.com

Prosper Mugare
Email Address: prosper.mugare@zw.ey.com

Tafadzwa Mavhunga
Email Address: tafadzwa.mavhunga@zw.ey.com

Carol Mucherahowa
Email Address: carol.mucherahowa@zw.ey.com

Andrew T Zigora
Email Address: andrew.zigora@zw.ey.com

Farisayi Kusangaya
Email Address: farisayi.kusangaya@zw.ey.com